CZĘŚĆ 8 SIWZ

SP.ZP.272.7.2018.II.FR

Dostawa i wdrożenie infrastruktury informatycznej dla Powiatu Wrocławskiego oraz 5 Gmin: Długołęki, Jordanowa Śląskiego, Kątów Wrocławskich, Mietkowa i Żórawiny", w podziale na 4 części.

Opis Przedmiotu Zamówienia
Część III - Dostawa infrastruktury sieciowej – aktywnej i pasywnej

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Dolnośląskiego 2014-2020; Oś Priorytetowa 2 Technologie Informacyjno - Komunikacyjne; Działanie 2.1 E-usługi publiczne, Poddziałanie 2.1.1 E-usługi publiczne – konkurs horyzontalny.

Opis Przedmiotu Zamówienia dla Części III składa się z 5 załączników:

1. Załącznik 8.1. do SIWZ – OPZ dla Części III – Powiat Wrocławski
2. Załącznik 8.2. do SIWZ – OPZ dla Części III – Gmina Jordanów Śląski
3. Załącznik 8.3. do SIWZ – OPZ dla Części III – Gmina Kąty Wrocławskie
4. Załącznik 8.4. do SIWZ – OPZ dla Części III – Gmina Mietków
5. Załącznik 8.5. do SIWZ – OPZ dla Części III – Gmina Żórawina

Wrocław, dnia 15.02. 2018 r.

Załącznik 8.1. do SIWZ – OPZ dla Części III – Powiat Wrocławski

1. **Zestawienie zbiorcze sprzętu w ramach części III - Dostawa infrastruktury sieciowej – aktywnej i pasywnej**

Część III – Dostawa infrastruktury sieciowej – aktywnej i pasywnej		**Powiat Wrocławski**
L.p.	**Rodzaj sprzętu**	**Ilość sztuk**
1.	Przełącznik rdzeniowy	3
2.	Przełącznik dostępowy	15
3.	Urządzenie brzegowe UTM	2
4.	Urządzenie do analizy ruchu - sieciowego	1
5.	Rozbudowa sieci dostępowej	2

2. **Wymagania generalne dla dostaw i usług związanych z niniejszą częścią zamówienia**

W zakresie realizacji niniejszych wymagań OPZ przewiduje się:

- Dostawę urządzeń teleinformatycznych w zakresie poz. 1 i 2 powyższej tabeli,
- Dostawę, instalację, konfigurację i uruchomienie poz. 3,4,5 zgodnie ze wskazaniem Zamawiającego urządzenia do analizy ruchu sieciowego, urządzeń dostępowych oraz urządzeń UTM.

Wszystkie wskazania z nazwy urządzeń występujących w szczegółowym opisie przedmiotu zamówienia należy rozumieć, jako określenie wymaganych minimalnych parametrów technicznych lub standardów jakościowych. Oznacza to, że zgodnie z art.29 ust.3 ustawy Prawo zamówień publicznych wskazaniom tym towarzyszą wyrazy „lub równoważne". Wykonawca, który w ofercie powoła się na zastosowanie urządzeń równoważnych opisanych w SIWZ, jest obowiązany wykazać, że oferowane urządzenia spełniają wymagania określone przez Zamawiającego.

3. **Wymagania szczegółowe minimalne dla sprzętu ujętego w ramach niniejszego przedmiotu zamówienia**

3.1. Rozbudowa infrastruktury sieciowej/Przełącznik rdzeniowy – 3 szt.

1. Przełącznik warstwy dostępowej z obsługą AP:
2. Przełącznik stackowalny wyposażony w 24 porty 10/100/1000BaseT
3. Przełącznik musi posiadać minimum jeden dodatkowy slot na moduł rozszerzeń z możliwością jego wymiany „na gorąco" (ang. hot swap). Wśród dostępnych modułów rozszerzeń muszą być dostępne co najmniej następujące moduły:
   a. Minimum 4-portowy moduł Gigabit Ethernet z gniazdami SFP
   b. Minimum 2-portowy moduł 10Gigabit Ethernet SFP+, przy czym wymagane jest, aby w przypadku wykorzystania pojedynczego łącza 10GE istniała możliwość instalacji dodatkowych 2 portów Gigabit Ethernet SFP

4. Porty SFP muszą umożliwiać ich obsadzenie modułami 1000Base-T, 1000Base-SX, 1000Base-LX/LH zależnie od potrzeb Zamawiającego. Porty SFP+ muszą umożliwiać ich obsadzenie modułami 10GBase-SR, 10GBase-LR, 10GBase-LRM oraz modułami optycznymi GE (1000Base-SX, 1000Base-LX/LH)
5. Przełącznik musi zapewniać możliwość stakowania z zapewnieniem następujących parametrów:
   a. Przepustowość w ramach stosu min. 480Gb/s
   b. Min. 9 urządzeń w stosie
   c. Zarządzanie poprzez jeden adres IP
   d. Możliwość tworzenia połączeń z kilku ethernetowych łączy fizycznych w jedno logiczne (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad
   e. Przełączniki muszą umożliwiać współdzielenie mocy zasilaczy tzn. zasilacze muszą stanowić zasób wspólny dla wszystkich przełączników w stosie (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE)
6. Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów
7. Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania. Zasilacze muszą być wymienne
8. Przełącznik musi posiadać możliwość rozbudowy o funkcję kontrolera sieci bezprzewodowej WiFi:
   a. Przełącznik musi zapewniać centralne zarządzanie punktami dostępowymi zgodnie z protokołem CAPWAP (RFC 5415), w tym zarządzane politykami bezpieczeństwa i zarządzanie pasmem radiowym (RRM) po zainstalowaniu odpowiedniej licencji
   b. Przepustowość dla sieci WiFi nie mniejsza niż 20Gb/s
   c. Obsługa minimum 2000 klientów sieci WiFi
   d. Możliwość terminowania tuneli CAPWAP na przełączniku (zapewnienie jednego punktu nakładania polityk QoS/bezpieczeństwa dla sieci LAN/WLAN)
9. Szybkość przełączania minimum 65Mpps dla pakietów 64-bajtowych
10. Minimum 4 GB pamięci DRAM i 2GB pamięci flash
11. Obsługa minimum :
    a. 1.000 sieci VLAN
    b. 32.000 adresów MAC
    c. 24.000 tras routingu
12. Obsługa protokołu NTP
13. Obsługa IGMPv1/2/3
14. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1w Rapid Spanning Tree
    b. IEEE 802.1s Multi-Instance Spanning Tree
15. Obsługa protokołu LLDP i LLDP-MED
16. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
17. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP
18. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    a. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)

b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
g. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
h. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www)
i. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
j. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
k. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)

19. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
a. Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
b. Implementacja co najmniej 4 kolejek dla ruchu wyjściowego dla sieci WLAN dla obsługi ruchu o różnej klasie obsługi
c. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek
d. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
e. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
f. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Możliwość skonfigurowania do 2000 ograniczeń per przełącznik
g. Kontrola sztormów dla ruchu broadcast/multicast/unicast
h. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

20. Wbudowane reflektometry (TDR) dla portów 10/100/1000
21. Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4 i IPv6 (minimum protokół RIP). Urządzenie musi zapewniać możliwość rozszerzenia funkcjonalności o wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, BGP) i IPv6 (OPSFv3), funkcjonalności Policy-based routingu i routingu multicast (PIM-SM, PIM-SSM) poprzez zakup odpowiedniej licencji lub wersji oprogramowania – bez konieczności dokonywania zmian sprzętowych
22. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)

23. Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 24.000 . Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow
24. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
25. Dedykowany port Ethernet do zarządzania out-of-band
26. Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
27. Urządzenie musi być wyposażone w port konsoli USB
28. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją
29. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
30. Możliwość montażu w szafie rack 19”. Wysokość urządzenia nie może przekraczać 1 RU
31. Urządzenie ma być dostarczone wraz z 2-portowym modułem 10Gigabit Ethernet SFP+ Multimode (wraz z dwoma wkładkami GBic, kablami do stackowania o długości 0,5m i patchcordami światłowodowymi (długość 5 m) do podłączenia serwerów Zamawiającego wyposażonych w złącze typu LC.

    Uwaga: Zamawiający w ramach infrastruktury sieciowej posiada urządzenia firmy CISCO. Nowe urządzenia powinny tworzyć jednolity system z już posiadanymi urządzeniami CISCO zgodny na poziomie protokołów oraz umożliwiający zarządzanie z jednego punktu (oprogramowania) już istniejącymi sieciami Vlan.). W zestawie wymagane jest dostarczenie dwóch kabli do stackowania.

    W wypadku dostarczenia innych urządzeń niż urządzenia marki CISCO wykonawca zapewni certyfikowane szkolenie (voucher/bon do wykorzystania w ciągu 1 roku, W ośrodku szkoleniowym na terenie Dolnego śląska) dla dwóch administratorów dotyczące dostarczonego rozwiązania. Ponadto zapewni wdrożenie i konfigurację systemu. A w wypadku braku zgodności dostarczonych urządzeń z powyższymi wymaganiami Wykonawca wymieni już posiadane przez Zamawiającego urządzenia na zgodne.

3.2. Rozbudowa infrastruktury sieciowej/Przełączniki dostępowe – 15 szt.

1. Typ i liczba portów:
   a. Minimum 24 portów 10/100/1000.
   b. Minimum 4 dodatkowe porty uplink 1 Gigabit Ethernet SFP.
   c. Porty SFP muszą umożliwiać ich obsadzanie wkładkami GigabitEthernet – minimum 1000Base- SX, 1000Base LX/LH, 1000Base-BX-D/U zależnie od potrzeb Zamawiającego.
2. Co najmniej 512MB pamięci DRAM oraz co najmniej 128MB pamięci Flash
3. Wielkość tablicy adresów MAC: co najmniej 16 000 .
4. Ilość obsługiwanych sieci VLAN: co najmniej 1 000
5. Wydajność:
   a. Przepustowość zapewniająca wydajność Line-rate
   b. Przełączanie dla pakietów 64-bajtowych: min. 71.4 Mpps.

6. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości co najmniej 9216 bajtów
7. Funkcjonalność urządzenia
   a. Obsługa co najmniej 16 statycznych tras dla routingu IPv4 i IPv6,
   b. Obsługa protokołu NTP,
   c. Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping,
   d. Możliwość uruchomienia funkcjonalności DHCP Server,
   e. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree – wymagane wsparcie dla min. 128 instancji protokołu STP,
   f. Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP),
   g. Musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP),
   h. Musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB,
   i. Musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli,
   j. Musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN),
   k. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych,
   l. Możliwość rozbudowy o funkcjonalność łączenia w stosy z zachowaniem następującej parametrów:
      - do min. 8 jednostek w stosie,
      - magistrala stakująca o przepustowości co najmniej 80Gb/s
      - możliwość tworzenia połączeń z kilku ethernetowych łączy fizycznych w jedno logiczne zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie
8. Bezpieczeństwo
   a. Minimum 4 poziomy dostępu administracyjnego poprzez konsolę,
   b. Autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL,
   c. Obsługa funkcji Guest VLAN,
   d. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
   e. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
   f. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie,
   g. Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6,
   h. Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) - zarówno dla IPv4 jak i IPv6,
   i. Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard,
   j. Funkcjonalność Protected Port,
   k. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego,

l. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne).

9. Wsparcie dla mechanizmów zapewnienia jakość usług w sieci
   a. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie co najmniej następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
   b. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek,
   c. Możliwość obsługi jednej z powyżej wymienionych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
   d. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi.
   e. 230V AC, możliwość zastosowania redundantnego zasilacza (dopuszcza się także rozwiązanie zewnętrzne)
10. Wysokość maksymalnie 1U, montowany w szafie typu RAC 19''
11. **Uwaga: Zamawiający w ramach infrastruktury sieciowej posiada urządzenia firmy CISCO. Nowe urządzenia powinny tworzyć jednolity system z już posiadanymi urządzeniami CISCO zgodny na poziomie protokołów oraz umożliwiający zarządzanie z jednego punktu (oprogramowania) już istniejącymi sieciami Vlan.).**

    W wypadku dostarczenia innych urządzeń niż urządzenia marki CISCO wykonawca zapewni certyfikowane szkolenie (voucher/bon do wykorzystania w ciągu 1 roku, W ośrodku szkoleniowym na terenie Dolnego Śląska) dla dwóch administratorów dotyczące dostarczonego rozwiązania. Ponadto zapewni wdrożenie i konfigurację systemu. A w wypadku braku zgodności dostarczonych urządzeń z powyższymi wymaganiami Wykonawca wymieni już posiadane przez Zamawiającego urządzenia na zgodne.

3.3. Urządzenie brzegowe UTM – 2 szt.

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.

- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active oraz Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dyski:

1. System realizujący funkcję Firewall musi dysponować minimum 20 portami Gigabit Ethernet RJ-45, 2 gniazdami SFP 1 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1,8 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 7 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps.
4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1,9 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES256-SHA1) dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

- Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
- Kontrola Aplikacji.
- Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
- Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
- Ochrona przed atakami - Intrusion Prevention System.
- Kontrola stron WWW.
- Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
- Zarządzanie pasmem (QoS, Traffic shaping).

- Analiza ruchu szyfrowanego protokołem SSL oraz SSH.
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
- Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

Polityki, Firewall

1. System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.
2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
4. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    - Wsparcie dla IKE v1 oraz v2.
    - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM)
    - Obsługa protokołu Diffiego-Hellman grup 19 i 20
    - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
    - Tworzenie połączeń typu Site-to-site oraz Client-to-Site.
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
    - Mechanizm „Split tunneling” dla połączeń Client-to-Site
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
    - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
    - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
3. Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej.
4. Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
    - Routingu statycznego

- Policy Based Routingu
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2800 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, Botnet.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, Dynamic DNS, proxy avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: np. Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie:

1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

- ICSA lub EAL4 dla funkcji Firewall

- ICSA lub NSS Labs dla funkcji IPS
- ICSA dla funkcji: SSL VPN, IPSec VPN

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres min. 36 miesięcy.
2. Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering, Sandbox, ochrona systemów mobilnych na okres min. 36 miesięcy.
3. Ochrona systemów przemysłowych SCADA na okres min. [36] miesięcy.
4. Logowanie do usługi realizowanej w chmurze na okres min.[36] miesięcy.
5. Możliwość weryfikacji poziomu bezpieczeństwa dla co najmniej 100 stacji klienckich na okres min 36 miesięcy .

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

Opisy do wymagań ogólnych.

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. **Uwaga: Zamawiający posiada 5 access pointów firmy Fortinet które muszą być zarządzane z poziomu UTM. W przypadku dostarczenia urządzeń innych niż marki Fortinet dostawca winien wymienić urządzenia dostępowe na zgodne z dostarczonymi urządzeniami UTM oraz zapewnić certyfikowane szkolenia dotyczącego tego rozwiązania dla 2 administratorów (voucher/bon do wykorzystania w ciągu 1 roku, W ośrodku szkoleniowym na terenie Dolnego Śląska).**

3.4. Urządzenie do analizy ruchu sieciowego – 1 szt.

System centralnego logowania, raportowania i korelacji logów

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej musi ono odpowiadać minimalnym wymaganiom jak dla platformy sprzętowej.

Dostarczone rozwiązanie musi w pełni współpracować z dostarczonymi urządzeniami brzegowymi UTM.

Interfejsy, Dyski:

1. System musi dysponować co najmniej 4 portami Gigabit Ethernet RJ-45 (nie dotyczy wersji programowej).
2. Rozwiązanie musi dysponować powierzchnią dyskową min. 1 TB (nie dotyczy wersji programowej).

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. System musi być w stanie przeanalizować minimum 120 logów na sekundę.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 150 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
    a. Listę najczęściej wykrywanych ataków.
    b. Listę najbardziej aktywnych użytkowników.
    c. Listę najczęściej wykorzystywanych aplikacji.
    d. Listę najczęściej odwiedzanych stron www.
    e. Listę krajów , do których realizowana jest komunikacja.
    f. Listę najczęściej wykorzystywanych polityk Firewall.
    g. Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów, co najmniej po typie logów (traffic, zdarzeń ataków, wykrycia malware'u, odwiedzanych stron, wykrytych aplikacji sieciowych).
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.

2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja Logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii eventów:
   - Malware.
   - Kontroli aplikacji.
   - Email.
   - IPS.
   - Traffic.
   - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
   a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
2. System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

   Oferent winien przedłożyć dokumenty:

   a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
   b) Certyfikat ISO 9001 podmiotu serwisującego.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla

utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

3. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

3.5. Rozbudowa sieci dostępowej wifi – 2 kpl.

Tryb pracy	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.
Obudowa	Kompaktowa obudowa z tworzywa sztucznego umożliwiającą montaż na suficie lub ścianie wewnątrz budynku.
Moduł radiowy	Musi być wyposażone w dwa niezależne moduły radiowe pracujące odpowiednio w pasmach: 5 GHz a/n/ac oraz 2,4 GHz b/g/n. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 14 SSID Przepustowość : • Dla radia 2,4 GHz: 300 Mbps • Dla radia 5 GHz: 867 Mbps Mechanizmy kolejkowania dla różnych klas ruchu: dane, voice, video Mechanizmy ochrony przed atakami na sieć radiową Wymagana moc nadawania min 20 dBm Mechanizmy uwierzytelniania 802.1x, w tym obsługa protokołów EAP: TLS, TTLS/MSCHAPv2, PEAP, GTC, SIM Możliwość tunelowania całej komunikacji do kontrolera sieci bezprzewodowych jak również funkcja bridge'owania ruchu z poszczególnych SSID do VLAN.
Anteny	Minimum 4 wbudowane anteny
Interfejsy	Interfejs sieciowy w standardzie 10/100/1000 Base-TX
Zasilanie	Możliwość zasilania w standardzie PoE 802.3af

W ramach postępowania powinien zostać dostarczony kontroler sieci bezprzewodowych, zarządzający planowaną strukturą urządzeń bezprzewodowych Access Point. Kontroler powinien oferować środowisko graficzne pozwalające na wykrywanie punktów dostępowych podpinanych do sieci a następnie na zarządzanie nimi.

Powinien umożliwiać zarządzanie grupą wskazanych przez Zamawiającego punktów dostępowych z możliwością rozbudowy do wartości docelowej.

4. Wymagania dotyczące gwarancji

Dostarczone, zainstalowane i uruchomione urządzenia mają być objęte przynajmniej 3-letnią gwarancją (chyba, że w formularzu ofertowym załączniku nr 1 Zamawiający wymaga innego okresu gwarancyjnego), świadczoną na miejscu u klienta z czasem reakcji serwisu - do końca następnego dnia roboczego. Okres gwarancji liczony będzie od dnia odbioru całego zainstalowanego i uruchomionego systemu. Szczegółowy zakres gwarancji został ujęty w SIWZ i w Umowie z wyłączeniem przełączników rdzeniowych i dostępowych. Przełączniki rdzeniowe i dostępowe należy dostarczyć z podstawową gwarancją producenta. Dostarczone przez Wykonawcę urządzenia zostaną podłączone do zasilania udostępnionego przez Zamawiającego.

Zamawiający dopuszcza zastosowanie urządzeń, technologii oraz programów równoważnych. Ciężar udowodnienia, że urządzenia oraz oferowana technologia jest równoważna w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy.

Urządzenia równoważne muszą pracować w tej samej technologii co urządzenia określone w dokumentacji.

Załącznik 8.2. do SIWZ – OPZ dla Części III – Gmina Jordanów Śląski

1. Stan obecny

Infrastruktura techniczna sieci komputerowej UG Jordanów Śląski (sieć szkieletowa) zapewnia niski poziom obsługi i wydajności. W roku 2004 wybudowana została sieć komputerowa obejmująca swoim zasięgiem Urząd Gminy Jordanów Śląski, składająca się m. in. z 305 m kabla UTP, gniazd natynkowych RJ 45 (puszka) w ilości 12 szt., wtyków RJ 45 w liczbie 30 szt.

Sieć komputerową wykonano według architektury wielowarstwowej, której szkielet oparty jest na przełącznikach sieciowych firmy Netgear oraz Digitus. Część pasywną sieci LAN stanowi system okablowania strukturalnego opartego na instalacji kat 5e, w którym nie ma fizycznego podziału na sieć wewnętrzną oraz zewnętrzną (dostępową do Internetu). Separację logiczną dostępu do sieci zewnętrznej Internet zapewniają urządzenia aktywne, tym samym korzystanie z dostępu do sieci Internet jest możliwe z każdego stanowiska pracy. Tak zbudowana sieć komputerowa dzieli się na podsieci, zapewniając w ten sposób bezpieczeństwo dla wydzielonych grup roboczych.

Wykorzystanie sieci komputerowej jest określone na poziomie ok 20% możliwości sieci. Ze względu na bardzo słabą jakość zastosowanych materiałów (kabel skrętka kat. 5e UTP, gniazd/modułów oraz wtyków RJ45) wiąże się to z niską wydajnością obecnej sieci tj. częste problemy z rozłączaniem grupy komputerów itp. Na 12 połączeń tylko niespełna 3 spełniają normę kat. 5e.

Serwery sprzętowe znajdują się w odseparowanej części sieci LAN z odpowiednimi regułami dostępu. Sieć podłączona jest do Internetu poprzez modem DSL następnie do routera głównego Netgear w szafie Rack. Obsługę sieci publicznej Internet zapewniają operatorzy lokalni, dostarczając łącze o przepustowości 10Mb/s. W obecnie funkcjonującej sieci stosowane są rozwiązania do monitorowania sieci. Również możliwe jest zdalne zarządzanie urządzeniami sieciowymi, jednak rozwiązanie to nie jest na co dzień stosowane. W szafie Rack serwerowej, która zlokalizowana jest w głównym budynku urzędu, znajdują serwery, spełniające następujące role/zadania:

a) ***serwer plików,***

b) ***Elektroniczny Obieg Dokumentów.***

Zabezpieczenie prądowe dla serwerów oraz urządzeń sieciowych gwarantuje centralny UPS EVER SINLINE 3000.

Z racji specyficznej struktury organizacyjnej (mała jednostka zaledwie z piętnastoma stanowiskami komputerowymi) i ograniczeń przestrzeni lokalowej aktualnie quasi-serwerownia zlokalizowana jest w szafie rakowej w jednym z biur. W stanie obecnym Gmina nie dysponuje wolnym pomieszczeniem, w którym istniałaby sposobność umiejscowienia serwerowni.

Stanowiska pracy w urzędzie są wyposażone w komputery osobiste (ok 15 szt.) o parametrach technicznych wymagających wymiany sprzętowej.

2. Ogólne wymagania

Wykonawca przed złożeniem oferty powinien dokonać wizji przedmiotowego obiektu i zapoznać się ze stanem i zakresem wcześniej wykonanych instalacji ze sporządzeniem ich inwentaryzacji dla celów złożenia oferty.

Wykonawca w ramach zamówienia zobowiązany jest dostarczyć projekt okablowania strukturalnego.

3. **Zestawienie zbiorcze sprzętu i usług w ramach części III - Dostawa infrastruktury sieciowej – aktywnej i pasywnej**

Część III – Dostawa infrastruktury sieciowej – aktywnej i pasywnej		**Gmina Jordanów Śląski**
L.p.	**Rodzaj sprzętu/usług**	**Ilość sztuk**
1.	Wykonanie projektu	1
2.	Wykonanie okablowania strukturalnego	1
3.	Dostawa i montaż klimatyzatora	1

4. **Wymagania generalne dla dostaw i usług związanych z niniejszą częścią zamówienia**

Podstawą do wykonania prac związanych z okablowaniem strukturalnym są normy okablowania strukturalnego. Normy europejskie dotyczące okablowania strukturalnego – wymagań ogólnych i specyficznych dla danego środowiska:

- ISO/IEC11801:2011 - Information technology - Generic cabling for customer premises
- PN-EN 50173-1:2011 Technika Informatyczna – Systemy okablowania strukturalnego - Część 1: Wymagania ogólne
- PN-EN 50173-2:2008/A1:2011E Technika Informatyczna – Systemy okablowania strukturalnego - Część 2: Budynki biurowe;

- Normy europejskie pomocnicze - w zakresie instalacji:
  - PN-EN 50174-1:2010/A1:2011E Technika informatyczna. Instalacja okablowania - Część 1 - Specyfikacja i zapewnienie jakości;
  - PN-EN 50174-2:2010/A1:2011E Technika informatyczna. Instalacja okablowania -Część 2 - Planowanie i wykonawstwo instalacji wewnątrz budynków;
  - PN-EN 50174-3:2005 Technika informatyczna. Instalacja okablowania -Część 3 - Planowanie i wykonawstwo instalacji na zewnątrz budynków;
  - PN-EN 50346:2004/A2:2010P Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania
  - PN-EN 50310:2012P Stosowanie połączeń wyrównawczych i uziemiających
- W przypadku powołań normatywnych niedatowanych obowiązuje zawsze najnowsze wydanie cytowanej normy.
- Wykonawca ma obowiązek wykonać instalację okablowania zgodnie z wymaganiami norm obowiązujących w czasie realizacji zadania, przy uwzględnieniu wszystkich wymagań opisanych w dokumentacji projektowej a zdefiniowane przez dokumenty wskazane powyżej.
- System okablowania oraz wydajność komponentów na etapie oddania instalacji do użytku musi pozostać w zgodzie z wymaganiami norm PN-EN50173-1:2011 i ISO/IEC11801:2011.

Wszystkie wskazania z nazwy urządzeń występujących w szczegółowym opisie przedmiotu zamówienia należy rozumieć, jako określenie wymaganych minimalnych parametrów technicznych lub standardów jakościowych. Oznacza to, że zgodnie z art.29 ust.3 ustawy Prawo zamówień publicznych wskazaniom tym towarzyszą wyrazy „lub równoważne”. Wykonawca, który w ofercie powoła się na zastosowanie urządzeń

równoważnych opisanych w SIWZ, jest obowiązany wykazać, że oferowane urządzenia spełniają wymagania określone przez Zamawiającego.

- **Wymagania szczegółowe minimalne dla usług i dostaw w ramach niniejszego przedmiotu zamówienia**

4.1. Projekt wykonawcy

1. Obowiązkiem przyszłego Wykonawcy po rozstrzygnięciu postępowania przetargowego jest przygotowanie kompletnej dokumentacji projektowej obejmujących wszystkie branże dla zadań opisanych w niniejszym OPZ. W poniższych punktach przedstawiono szczegółowe wytyczne do przygotowania dokumentacji projektowych.
2. W projekcie wykonawczym Wykonawca powinien wyszczególnić wszystkie niezbędne roboty budowlane i instalacyjne wraz z niezbędnymi ekspertyzami dotyczącymi niniejszego projektu, o ile takie są konieczne.
3. Projekt powinien zawierać:
    a. specyfikację materiałową,
    b. rysunki (plany) lokalizacji głównych elementów okablowania, prowadzenia tras kablowych,
    c. rysunki szaf,
    d. trasę krosowania i oznaczenia gniazd.
4. Dokumentacja projektowa powinna umożliwiać etapową realizację prac, pozwalając w trakcie tych prac na bezpieczne użytkowanie istniejącego sprzętu informatycznego.
5. Zabezpieczenia, o których mowa w niniejszym dokumencie, powinny uwzględniać ochronę przed czynnikami losowymi oraz przed nieumyślnym i umyślnym działaniem człowieka. W dokumentacjach projektowych należy więc założyć współdziałanie systemów infrastruktury, systemów informatycznych i procedur administracyjnych.
6. Dokumentacja projektowa musi być wykonane oraz zatwierdzone przez wykwalifikowany personel posiadający właściwe uprawnienia projektowe z danej branży oraz aktualny wpis do Okręgowej Izby Inżynierów Budownictwa. Kopię właściwych uprawnień oraz Wpis do Okręgowej Izby Inżynierów Budownictwa należy zamieścić w dokumentacji projektowej.
7. Wszystkie rysunki winny być podpisane przez projektanta i sprawdzającego.
8. Bazą do przygotowania dokumentacji projektowej są dołączone jako załączniki do niniejszego OPZ rysunki o numerach 1, 2, 3, 4, 5.
9. Dokumentację projektową należy przygotować w 3 egzemplarzach w wersji papierowej oraz 1 wersji elektronicznej na płycie DVD.
10. Projekt mus być opracowywany w porozumieniu z Zamawiającym, przez niego zatwierdzone oraz pisemnie dopuszczony do realizacji.

4.2. Okablowanie strukturalne

Wykonanie okablowania strukturalnego musi zostać wykonane zgodnie z wymienionymi poniżej wymaganiami:

1. Kable ekranowane w standardzie kategorii 6.
2. Wymagany interfejs w zespole gniazda natynkowego (naściennego) – RJ 45 o wydajności kat. 6, pozwalający na wykorzystanie standardowych kabli przyłączeniowych RJ45/Rj45.

3. Zastosowane gniazda logiczne RJ-45 muszą być nierozłączne, tj. w jednym module złącze terminacji kabla i część gniazda RJ 45 (bez wymiennych wkładek wprowadzających dodatkowe złącze w gnieździe). Terminacja kabla w złączu powinna być zgodna z normą na okablowanie, odpowiednio np. PN-EN 50173 lub ISO 11801 w sekwencji 568 B dla każdego gniazda RJ 45 wszystkich 4 par kabla (niedopuszczalne jest wykorzystanie gniazd 2 x RJ 45 na jednym przewodzie UTP) na złączu LSA.
4. Panele ekranowane muszą zawierać gniazda projektowane na płytkach PCB, celem lepszej eliminacji przesłuchów pomiędzy gniazdami, terminacja ekranu w złączu LSA, dodatkowo panel wyposażony w metalowe półokrągłe uchwyty mocujące przewód i zapewniające dodatkowe podłączenie i uziemienie ekranu kabla; panel standardowo powinien być w przewód uziemiający, a złącza muszą być chronione przed kurzem poprzez zamykaną metalową obudowę.
5. Kable transmisyjne, zgodnie z normą, powinny być zakończone w sposób trwały na ośmiopozycyjnym złączu.
6. Maksymalna długość przewodu instalacyjnego (od punktu dystrybucyjnego do gniazda końcowego) wynosi ok. 915 m.
7. Gniazda muszą zostać ponumerowane w sposób trwały i widoczny, według następującego schematu: NN-PPP na patchpanelu w punkcie dystrybucyjnym oraz NN w punkcie końcowym, gdzie PPP to numer pokoju, a NN to numer gniazda.
8. Trzyletni okres gwarancji liczony jest od dnia, w którym podpisano protokół odbioru.
9. W celu weryfikacji zainstalowanego symetrycznego miedzianego okablowania strukturalnego na zgodność parametrów z normami należy przeprowadzić pomiary odpowiednim miernikiem przeznaczonym do certyfikacji sieci.
10. Wszystkie stosowane materiały i urządzenia muszą być fabrycznie nowe i wysokiej jakości, a także muszą dokładnie odpowiadać warunkom niezbędnym do prawidłowego wykonania powierzonych robót oraz do poprawnego funkcjonowania całej instalacji.
11. Wykonawca dostarczy okablowanie strukturalne szacowane na ok. 15 gniazd natynkowych.
12. Ze względu na warunki budowy i status obiektu okablowanie poziome zostanie rozprowadzone w korytarzach oraz w pomieszczeniach, do punktu logicznego – nadtynkowo lub w kanałach kablowych.
13. Wszystkie tory kablowe powinny być wykonane z wykorzystaniem listew instalacyjnych z PCW, w sposób pozwalający na zachowanie odpowiednich promieni gięcia wiązek kablowych na zakrętach.
14. Zamawiający nie dopuszcza montażu torów kablowych na żadnym z odcinków na kleje tynkowe, a jedynie z wykorzystaniem kołków montażowych.
15. Zamawiający nie zezwala na przeciąganie przewodów toru kablowego przez przepusty ścianowe i międzystropowe – bez wprowadzania w nie peszli sztywnych PCV.
16. Wykonawca, prowadząc tory kablowe dla sieci strukturalnej zobligowany jest do zachowania szczególnej ostrożności w trakcie realizacji odwiertów przez ściany działowe lub międzystropowe w zakresie istniejących instalacji elektrycznych, których położenie w obiekcie nie jest udokumentowane schematem instalacyjnym.
17. Wszelki uszkodzenia infrastruktury ogólne w budynku spowodowane przez Wykonawcę podczas prowadzenia prac instalacyjnych obciążają jego samego i muszą być usunięte w ramach nieodpłatnego usunięcia szkód w terminie natychmiastowym, po ich stwierdzeniu.
18. Zamawiający wymaga, aby odpady powstałe w wyniku realizowanych robót budowlanych, jak i niebezpieczne narzędzia i inne przedmioty były każdorazowo uprzątnięte z ciągów komunikacyjnych do

godz. 7.30 tak, aby umożliwiały bezpieczne przemieszczanie się pracowników w godzinach pracy Urzędu.

19. Wykonawca zobowiązany jest do pozostawienia pomieszczeń, w których będą wykonywane prace w stanie takim, jaki zastał przed przystąpieniem do prac.

4.3. Klimatyzator

L.p.	**Opis przedmiotu/funkcji/parametrów**	**Opis parametrów oferowanego towaru**
1.	Komplet klimatyzacji inwerterowej wraz ze wspornikiem.	
1.1	Wymiary: WxSxG (mm): 890 x 880 x 370 ,	
1.2	waga (kg): 44,	
1.3	użytkownik ma do wyboru jeden z kilku trybów pracy: chłodzenie, osuszanie, grzanie i wentylacja pomieszczenia.	
2.	Jednostka wewnętrzna:	
2.1	automatyczna regulacja kierunku nawiewu w pionie,	
2.2	ręczna regulacja kierunku nawiewu w poziomie,	
2.3	wyświetlacz trybu pracy urządzenia,	
2.4	wyświetlacz temperatury,	
2.5	filtr mechaniczny, przeciwpyłowy,	
2.6	przepływ powietrza (m3/h) 650,	
2.7	poziom ciśnienia akustycznego (db(A)) od 32 do 40,	
2.8	temperaturowy zakres nastawy urządzenia (°C) od +16 do +31,	
2.9	wymiary: WxSxG (mm) 280 x 799 x 183	
2.10	waga (kg) 10	
3.	Jednostka zewnętrzna:	
3.1	wydajność podczas chłodzenia (kW) 3,5,	
3.2	wydajność podczas grzania (kW) 3,5,	
3.3	pobór mocy podczas chłodzenia (kW) 1,08 (od 0,29 do 1,33),	
3.4	pobór mocy podczas grzania (kW) 0,94 (od 0,29 do 1,7),	
3.5	klasa energetyczna - chłodzenie A++,	
3.6	klasa energetyczna - grzanie A+,	
3.7	SEER 6,1,	
3.8	SCOP 4,0,	
3.9	poziom ciśnienia akustycznego (dB(A)) od 48 do 52,	
3.10	temperaturowy zakres pracy urządzenia (°C) od -15 do +48,	
3.11	maksymalna długość instalacji freonowej (m) 15 m	
3.12	maks. różnica wysokości pomiędzy jednostkami (m) 5,	
3.13	średnice rur freonowych ciecz/gaz (mm) 6,35/9,52,	
3.14	czynnik chłodniczy R410A,	
3.15	zasilanie 230V, 50Hz,	
3.16	wymiary WxSxG (mm) 551 x 760 x 256,	

3.17	Urządzenie obsługuje Private VLANs (across switches).	
3.18	waga (kg) 32.	
4.	Pilot, sterownik:	
4.1	timer,	
4.2	tryb ekonomiczny,	
4.3	tryb pełnej mocy,	
4.4	tryb ustawień nocnych,	
4.5	zasilanie bateryjne TAK, AAA - 2 szt.	

5. Wymagania dotyczące gwarancji

Dostarczone, zainstalowane i uruchomione urządzenia mają być objęte przynajmniej 3-letnią gwarancją (chyba, że w formularzu ofertowym załączniku nr 1 Zamawiający wymaga innego okresu gwarancyjnego), świadczoną na miejscu u klienta z czasem reakcji serwisu - do końca następnego dnia roboczego.

Okres gwarancji liczony będzie od dnia odbioru całego zainstalowanego i uruchomionego systemu. Szczegółowy zakres gwarancji został ujęty w SIWZ i w Umowie.

Dostarczone przez Wykonawcę urządzenia zostaną podłączone do zasilania udostępnionego przez Zamawiającego.

Zamawiający dopuszcza zastosowanie urządzeń, technologii oraz programów równoważnych innych niż określone w SIWZ. Ciężar udowodnienia, że urządzenia oraz oferowana technologia jest równoważna w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy.

Urządzenia równoważne muszą pracować w tej samej technologii co urządzenia określone w dokumentacji.

Załączniki:

1. Rysunek nr 1 do Załącznika 8.2. do SIWZ – OPZ dla Części III – Gmina Jordanów Śląski
2. Rysunek nr 2 do Załącznika 8.2 do SIWZ – OPZ dla Części III – Gmina Jordanów Śląski
3. Rysunek nr 3 do Załącznika 8.2. do SIWZ – OPZ dla Części III – Gmina Jordanów Śląski
4. Rysunek nr 4 do Załącznika 8.2. do SIWZ – OPZ dla Części III – Gmina Jordanów Śląski
5. Rysunek nr 5 do Załącznika 8.2. do SIWZ – OPZ dla Części III – Gmina Jordanów Śląski

Załącznik 8.3. do SIWZ – OPZ dla Części III – Gmina Kąty Wrocławskie

1. **Zestawienie zbiorcze sprzętu w ramach części III - Dostawa infrastruktury sieciowej – aktywnej i pasywnej**

Część III – Dostawa infrastruktury sieciowej – aktywnej i pasywnej		Gmina Kąty Wrocławskie
L.p.	**Rodzaj sprzętu**	**Ilość sztuk**
1.	Przełącznik dostępowy	3
2.	UTM	3

2. **Wymagania generalne dla dostaw i usług związanych z niniejszą częścią zamówienia**

   W zakresie realizacji niniejszych wymagań OPZ przewiduje się:

   - Dostawę, instalację, konfigurację i uruchomienie zgodnie ze wskazaniem Zamawiającego urządzeń wymienionych w poz. 1 i 2 powyższej tabeli.

   Wszystkie wskazania z nazwy urządzeń występujących w szczegółowym opisie przedmiotu zamówienia należy rozumieć, jako określenie wymaganych minimalnych parametrów technicznych lub standardów jakościowych. Oznacza to, że zgodnie z art.29 ust.3 ustawy Prawo zamówień publicznych wskazaniom tym towarzyszą wyrazy „lub równoważne". Wykonawca, który w ofercie powoła się na zastosowanie urządzeń równoważnych opisanych w SIWZ, jest obowiązany wykazać, że oferowane urządzenia spełniają wymagania określone przez Zamawiającego.

3. **Wymagania szczegółowe minimalne dla sprzętu ujętego w ramach niniejszego przedmiotu zamówienia**

   3.1. ***Urządzenie UTM Typ 1 – 2 szt.***

   Dostarczony system bezpieczeństwa (dostarczane urządzenie wraz z niezbędnym oprogramowaniem), musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

   Dla elementów systemu bezpieczeństwa obsługujących niniejszy podmiot, Wykonawca zapewni wszystkie poniższe funkcje i parametry pracy:

   1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.
   2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   3. Monitoring stanu realizowanych połączeń VPN.
   4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
   5. System realizujący funkcję Firewall powinien dysponować minimum 16 portami Ethernet 10/100/1000 Base-TX

6. System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
7. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę
8. Przepustowość Firewall'a: nie mniej niż 7 Gbps
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 4 Gbps
10. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 480 GB. System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
11. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.
12. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
    - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
    - Ochrona przed atakami - Intrusion Prevention System
    - Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
    - Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
    - Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
    - Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)
    - Możliwość analizy ruchu szyfrowanego protokołem SSL
    - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
    - Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych
13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 1,5 Gbps
14. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 250Mbps
15. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
    - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    - Praca w topologii Hub and Spoke oraz Mesh
    - Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
16. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

18. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
19. Translacja adresów NAT adresu źródłowego i docelowego.
20. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
21. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
22. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
23. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
24. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
25. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
26. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
27. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:
    - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    - haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
    - Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
28. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

- ICSA lub EAL4 dla funkcji Firewall
- ICSA lub NSS Labs dla funkcji IPS
- ICSA dla funkcji: SSL VPN, IPSec VPN

29. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
30. Serwisy i licencje
    - W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 36 miesięcy.
31. Gwarancja oraz wsparcie

1) Gwarancja: System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia

w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.

2) Gwarancja/AHB/SOS: System powinien być objęty rozszerzonym serwisem gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin/, realizowanym przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego, mającego swoją siedzibę na terenie Polski.

   Dla zapewnienia wysokiego poziomu usług podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w trybie 8x5 / 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię 8x5 /24x7.

   Oferent winien przedłożyć dokumenty:

   - oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej
   - oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej)
   - certyfikat ISO 9001 podmiotu serwisującego

3) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

4) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

32. Instalacja, konfiguracja i wdrożenie w siedzibie Zamawiającego na podstawie wytycznych i polityk przekazanych przez przedstawicieli Zamawiającego

33. **Uwaga: Zamawiający w ramach infrastruktury sieciowej posiada urządzenie do analizy ruchu sieciowego firmy Fortinet, które będzie wykorzystywane z dostarczanymi urządzeniami UTM. W przypadku dostarczenia urządzeń innych niż marki Fortinet dostawca winien wymienić urządzenie do analizy ruchu sieciowego na zgodne z dostarczonymi urządzeniami UTM oraz zapewnić certyfikowane szkolenia dotyczącego tego rozwiązania dla 2 administratorów.**

3.2. Urządzenie UTM Typ 2 – 1 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa obsługujących niniejszy podmiot, Wykonawca zapewni wszystkie poniższe funkcje i parametry pracy:

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
5. System realizujący funkcję Firewall powinien dysponować minimum 10 portami Ethernet 10/100/1000 Base-TX
6. System powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
7. W zakresie Firewall'a obsługa nie mniej niż 1,2 mln. jednoczesnych połączeń oraz 28 tys. nowych połączeń na sekundę
8. Przepustowość Firewall'a: nie mniej niż 3 Gbps
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 1600 Mbps
10. System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
11. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.
12. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
    - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
    - Ochrona przed atakami - Intrusion Prevention System
    - Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
    - Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
    - Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
    - Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)

- Możliwość analizy ruchu szyfrowanego protokołem SSL
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
- Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.

13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 1200 Mbps
14. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 180 Mbps
15. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
    - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    - Praca w topologii Hub and Spoke oraz Mesh
    - Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
16. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
18. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
19. Translacja adresów NAT adresu źródłowego i docelowego.
20. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
21. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
22. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
23. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
24. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
25. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
26. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
27. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:
    - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    - haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych

- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory

28. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
    - ICSA lub EAL4 dla funkcji Firewall
    - ICSA lub NSS Labs dla funkcji IPS
    - ICSA dla funkcji: SSL VPN, IPSec VPN
29. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
30. Serwisy i licencje
    - W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 36 miesięcy.
31. Gwarancja oraz wsparcie

1) Gwarancja: System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.
2) Gwarancja/AHB/SOS: System powinien być objęty rozszerzonym serwisem gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin/, realizowanym przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego, mającego swoją siedzibę na terenie Polski.

   Dla zapewnienia wysokiego poziomu usług podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w trybie 8x5 / 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię 8x5 /24x7.

   Oferent winien przedłożyć dokumenty:
   - oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej
   - oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej)
   - certyfikat ISO 9001 podmiotu serwisującego
3) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla

utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

4) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

32. Instalacja, konfiguracja i wdrożenie w siedzibie Zamawiającego na podstawie wytycznych i polityk przekazanych przez przedstawicieli Zamawiającego.

33. **Uwaga: Zamawiający w ramach infrastruktury sieciowej posiada urządzenie do analizy ruchu sieciowego firmy Fortinet, które będzie wykorzystywane z dostarczanymi urządzeniami UTM. W przypadku dostarczenia urządzeń innych niż marki Fortinet dostawca winien wymienić urządzenie do analizy ruchu sieciowego na zgodne z dostarczonymi urządzeniami UTM oraz zapewnić certyfikowane szkolenia dotyczącego tego rozwiązania dla 2 administratorów.**

3.3. Przełącznik sieciowy – switch – 3 szt.

L.p.	**Opis przedmiotu/funkcji/parametrów**	**Opis parametrów oferowanego towaru**
1.	Przełącznik musi posiadać architekturę umożliwiającą przełączanie w warstwie 2 ethernet i 3 ipv4 oraz ipv6.	
2.	Przełącznik musi być wyposażony w poniższe porty	
2.1	co najmniej 48 portów dostępowych Ethernet 10/100/1000Base-T IEEE 802.3z Auto-MDI/MDIX	
2.2	co najmniej 4 porty uplink 10 Gigabit Ethernet SFP+, obsługujące co najmniej moduły SFP TX, SX, LX/LH, LH/ZX, zgodne ze standardem IEEE 802.3z, oraz SFP+ LR,SR.	
2.3	Każdy przełącznik musi być wyposażony w: 3 moduły SFP+ LR 10km w pełni kompatybilny z modułami oferowanymi przez producenta przełącznika wraz z obsługą funkcjonalności DOM (pomiar temperatury, prądu i mocy sygnału optycznego; 1 moduł SFP+ 10-Gigabit Ethernet Direct Attach do długości min 3m; 2 kabele krosowe FO SC-LC o długości 5m; 1 kabel krosowy FO LC-LC o długości 5m	
2.4	Wszystkie porty muszą pracować z pełną prędkością interfejsów (wire-speed) dla pakietów dowolnej wielkości, czyli przełącznik musi mieć wydajność ponad 100 Mpps (130 Mpps łącznie z portami stackującymi).	
3.	Przełącznik jest dedykowanym urządzeniem sieciowym o wysokości 1U, przystosowanym do montażu w szafie rack 19'' oraz posiada oprzyrządowanie niezbędne do zamocowania w takiej szafie.	
4.	Przełącznik musi być wyposażony w minimum jeden zasilacz AC, przystosowany do zasilania z sieci 230V/50Hz.	
5.	Przełączniki muszą posiadać możliwość łączenia w stos, tak że 10	

	przełączników jest widocznych w sieci jako jedno urządzenie bez utraty wymaganych funkcjonalności. Każdy switch musi posiadać co najmniej 2 porty stackujące o przepustowości nie mniejszej niż 10 Gb/s każdy, jednocześnie w obie strony; oraz co najmniej jeden kabel stackujący o długości nie mniejszej niż 50 cm.	
6.	Przełącznik obsługuje co najmniej 16000 adresów MAC, w tym co najmniej 1000 adresów MAC opisanych statycznie w konfiguracji.	
7.	Przełącznik obsługuje sieci VLAN zgodnie z IEEE 802.1Q w ilości nie mniejszej niż 1000 z zakresu 1-4090 VLAN ID oraz protokół MVRP.	
8.	Urządzenie obsługuje agregowanie połączeń zgodnie z IEEE 802.3AD, nie mniej niz 6 grup LACP do 8 portów każda. Przy wysyłaniu pakietu IP przez interfejs LACP do wyznaczenia fizycznego portu na który pakiet będzie wysłany jest brany pod uwagę co najmniej adres IP źródłowy i docelowy tego pakietu, w przypadku protokołów TCP i UDP również numery portów, a dla innych protokołów co najmniej adres źródłowy i docelowy, lub źródłowe i docelowe adresy MAC.	
9.	Urządzenie obsługuje filtrowanie ruchu wejściowego i wyjściowego co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4 IPv4 (pole TTL protokołu IP może być obsługiwane tylko przy filtrowaniu ruchu wejściowego na interfejsach warstwy 3). Urządzenie realizuje sprzętowo nie mniej niż 500 reguł filtrowania ruchu. Jest dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.	
10.	Przełącznik obsługuje ramki jumbo (9216 bajtów) na wszystkich interfejsach.	
11.	Przełącznik jest przystosowany do pracy ciągłej przy temperaturze otoczenia z zakresu 0 – 45^{o}C.	
12.	Przełącznik jest wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania	
13.	Przełącznik umożliwia wgranie systemu operacyjnego z zewnętrznego nośnika danych poprzez łącze szeregowe RS-232, USB lub dedykowany port ethernetowy. Musi istnieć możliwość ustawienia restartu urządzenia w zadanym terminie.	
14.	Zarządzanie urządzeniem musi być możliwe za pośrednictwem interfejsu linii komend (CLI) przez port konsoli oraz zdalnie przez telnet lub ssh przy użyciu zarówno protokołu IPv4 jak i IPv6.	
15.	Urządzenie umożliwia zapisanie aktualnej konfiguracji w postaci tekstowej (może być skompresowana jeśli istnieje niezależny, bezpłatny program do jej rozpakowania) w wewnętrznej pamięci nieulotnej oraz na urządzeniach zewnętrznych przy pomocy protokołu tftp, ftp lub scp. Istnieje możliwość modyfikowania konfiguracji poza urządzeniem i ponownego jej wczytania do urządzenia.	
16.	Przełącznik generuje logi dotyczące zdarzeń na nim zachodzących. Użytkownik ma dostęp do dokumentacji producenta urządzenia z	

	wyjaśnieniami znaczenia poszczególnych wpisów w logach. Logi te są dostępne lokalnie na urządzeniu oraz przesyłane do innych urządzeń z użyciem protokołu syslog (przy użyciu protokołu ipv4 lub ipv6, zależnie od konfiguracji dokonanej przez użytkownika). Istnieje możliwość uszczegóławiania logów (tryb debug) dotyczących konkretnych usług (np. STP, 802.1x itp.)	
17.	Przełącznik umożliwia ustawienie limitów pakietów akceptowanych na wskazanych portach w jednostce czasu (tzw. rate-limit). Przełącznik odrzuca pakiety przekraczające limit. Istnieje możliwość ustawiania limitów pakietów indywidualnie dla każdego interfejsu.	
18.	Przełącznik umożliwia ustawienie limitów pakietów typu broadcast oraz unknown unicast w jednostce czasu indywidualnie na każdym interfejsie. Przełącznik odrzuca pakiety przekraczające zadany limit.	
19.	Urządzenie umożliwia dynamiczne przyporządkowywanie komputerów do VLANu na podstawie adresu MAC (tzw. dynamic vlans lub MAC based vlans).	
20.	Urządzenie obsługuje Private VLANs (across switches).	
21.	Urządzenie obsługuje protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9.	
22.	Urządzenie udostępnia za pomocą protokołu SNMP i interfejsu CLI co najmniej 64 bitowe liczniki ramek i bajtów wysłanych i odebranych na poszczególnych portach. Ponadto istnieje możliwość obsługi liczników odebranych ramek zawierających błędy na poszczególnych interfejsach oraz liczniki ramek których nie udało się wysłać lub wystąpiły błędy podczas ich wysyłania.	
23.	Dostępna jest funkcja kopiowania (mirroring) ruchu dla pakietów spełniających warunki określone w odpowiednim filtrze.	
24.	Urządzenie posiada możliwość diagnostyki kabla, TDR (Time Domain Reflectometer) na wszystkich portach 10/100/1000BASE-T. Urządzenie pozwala na konfigurowanie maksymalnej, rozgłaszanej w czasie autonegocjacji, prędkości portu w standardzie 10/100/1000BASE-T.	
25.	Przełącznik umożliwia zdefiniowanie czasu po jakim będzie próbował aktywować porty wyłączone automatycznie ze względu na nieprawidłowości występujące w przyłączonych do nich częściach sieci (errdisable recovery).	
26.	Przełącznik posiada funkcjonalność netFlow, netflow lite lub równoważną (np. RFC3176 sFlow) umożliwiającą monitorowanie ruchu w warstwach 3 do 4 modelu OSI dla pakietów IPv4.	
27.	Przełącznik obsługuje protokół Spanning Tree i Rapid Spannig Tree, a także Multiple Spanning Tree (nie mniej niż 16 instancji MSTP) oraz VLAN Spanning Tree Protocol (lub równoważny) dla co najmniej 128 vlan-ów.	

28.	Przełącznik posiada możliwość wyłączenia Spanning Tree oraz filtrowania (ignorowania) ramek BPDU na wskazanych portach.	
29.	Przełącznik udostępnia informacje dla każdej instancji SPT, kiedy przyszedł ostatni pakiet TCN (Topology Change Notification) oraz liczniki pakietów TCN dla każdej instancji SPT lub informację z którego interfejsu przyszedł ostatni pakiet TCN.	
30.	Switch posiada opcję definiowania zapasowego portu dla portu podstawowego, tzn. tylko jeden z dwóch interfejsów jest aktywny w danej chwili	
31.	Przełącznik obsługuje protokół LLDP i LLDP-MED, w tym przydział numeru VLANu i klasy QOS dla telefonów VoIP.	
32.	Urządzenie posiada mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu może odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1P), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie obsługuje sprzętowo nie mniej niż 8 kolejek na port fizyczny, w tym możliwość zdefiniowania co najmniej jednej kolejki jako kolejki priorytetowej (strict priority) oraz co najmniej jedna kolejka umożliwia pracę w trybie shaping (wygładzania ruchu).	
33.	Przełącznik obsługuje IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie, autoryzowanych każdy indywidualnie. Przełącznik przypisuje ustawienia dla użytkownika na podstawie atrybutów (co najmniej VLAN oraz reguła filtrowania ruchu) zwracanych przez serwer RADIUS, dostępny zarówno przez ipv4 jak i ipv6. Istnieje możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik wspiera co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.	
34.	Przełącznik umożliwia określanie maksymalnej liczby adresów MAC dopuszczalnych na wskazanym porcie. Po przekroczeniu limitu dopuszczalnych adresów MAC pakiety z adresami źródłowymi MAC nie znajdującymi się w zbudowanej tablicy MAC będą ignorowane.	
35.	Przełącznik obsługuje protokół MVR (Multicast VLAN Registration).	
36.	Przełącznik obsługuje sprzętowo takie mechanizmy bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, IP Source Guard, DHCP Snooping (wraz z obsługą opcji 82), dla protokołu ipv4 i ich odpowiedniki w protokole ipv6, tzn. Negihbor Discover Inspection oraz filtruje Router Advertisements na niezaufanych portach.	
37.	Przełącznik posiada funkcjonalność IGMP (v2, v3) oraz MLD (v1 i v2) snooping i wysyła ramki multicastowe tylko do nasłuchujących klientów. Funkcjonalność ta nie zakłóca poprawnej pracy multicastów IPv6, w tym standardu Neighbor Discovery.	

38.	Przełącznik musi obsługiwać co najmniej 500 tras routingu unicast ipv4 i 500 tras unicast ipv6 jednocześnie, co najmniej 200 pozycji ARP i 500 tras multicast ipv4/IGMP groups i ipv6. Przełącznik potrafi pracować w trybie proxy ARP oraz wykonywać DHCP relay na zadanych interfejsach.	
39.	Urządzenia muszą być nieużywane, fabrycznie nowe, tzn. nie starsze niż 6 miesięcy i nie przewidziane do wycofania z produkcji, pochodzić z legalnych kanałów dystrybucji producenta sprzętu. Urządzenia muszą posiadać dożywotnią gwarancję producenta (tzn. co najmniej 3 lat od momentu ogłoszenia terminu zakończenia produkcji). Pomoc techniczna oraz szkolenia z produktu muszą być świadczone w języku polskim. Nowe krytyczne aktualizacje wersji firmware muszą być ogólnodostępne lub Zamawiający musi mieć zapewniony dostęp do nowych wersji oprogramowania przez co najmniej 5 lat od podpisania protokołu odbioru. Zamawiający musi mieć zapewniony dostęp do wszystkich instrukcji użytkownika opublikowanych przez producenta urządzenia oraz dokumentacji do modułów i oprogramowania dostarczonego w ramach realizacji zamówienia. Zamawiający musi mieć możliwość zgłaszania Producentowi błędów w działaniu oprogramowania urządzenia oraz możliwość pobierania poprawek poprzez oficjalne kanały wsparcia.	
40.	Dopuszcza się aby wymagane standardy były obsługiwane w wersjach nowszych niż wymienione powyżej.	
41.	**Uwaga: Zamawiający w ramach infrastruktury sieciowej posiada urządzenia firmy JUNIPER. Nowe urządzenia powinny tworzyć jednolity system z już posiadanymi urządzeniami JUNIPER zgodny na poziomie protokołów oraz umożliwiający zarządzanie z jednego punktu (oprogramowania) już istniejącymi sieciami Vlan.). W wypadku dostarczenia innych urządzeń niż urządzenia marki JUNIPER wykonawca zapewni certyfikowane szkolenie (voucher/bon do wykorzystania w ciągu 1 roku, w ośrodku szkoleniowym na terenie Dolnego Śląska) dla dwóch administratorów dotyczące dostarczonego rozwiązania. W wypadku braku zgodności dostarczonych urządzeń z powyższymi wymaganiami Wykonawca wymieni już posiadane przez Zamawiającego urządzenia na zgodne.**	

4. **Wymagania dotyczące gwarancji**

Dostarczone, zainstalowane i uruchomione urządzenia mają być objęte przynajmniej 3-letnią gwarancją (chyba, że w formularzu ofertowym załączniku nr 1 Zamawiający wymaga innego okresu gwarancyjnego), świadczoną na miejscu u klienta z czasem reakcji serwisu - do końca następnego dnia roboczego.

Okres gwarancji liczony będzie od dnia odbioru całego zainstalowanego i uruchomionego systemu. Szczegółowy zakres gwarancji został ujęty w SIWZ i w Umowie.

Dostarczone przez Wykonawcę urządzenia zostaną podłączone do zasilania udostępnionego przez Zamawiającego.

Zamawiający dopuszcza zastosowanie urządzeń, technologii oraz programów równoważnych innych niż określone w SIWZ. Ciężar udowodnienia, że urządzenia oraz oferowana technologia jest równoważna w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy.

Urządzenia równoważne muszą pracować w tej samej technologii co urządzenia określone w dokumentacji.

Załącznik 8.4. do SIWZ – OPZ dla Części III – Gmina Mietków

1. **Zestawienie zbiorcze sprzętu w ramach części III - Dostawa infrastruktury sieciowej – aktywnej i pasywnej**

Część III – Dostawa infrastruktury sieciowej – aktywnej i pasywnej		**Gmina Mietków**
L.p.	**Rodzaj sprzętu**	**Ilość sztuk**
1.	Switch zarządzalny	1
2.	Firewall	1

2. **Wymagania generalne dla dostaw i usług związanych z niniejszą częścią zamówienia**

W zakresie realizacji niniejszych wymagań OPZ przewiduje się:

- Dostawę, instalację, konfigurację i uruchomienie zgodnie ze wskazaniem Zamawiającego urządzeń wymienionych w poz. 1 i 2 powyższej tabeli.

Wszystkie wskazania z nazwy urządzeń występujących w szczegółowym opisie przedmiotu zamówienia należy rozumieć, jako określenie wymaganych minimalnych parametrów technicznych lub standardów jakościowych. Oznacza to, że zgodnie z art.29 ust.3 ustawy Prawo zamówień publicznych wskazaniom tym towarzyszą wyrazy „lub równoważne". Wykonawca, który w ofercie powoła się na zastosowanie urządzeń równoważnych opisanych w SIWZ, jest obowiązany wykazać, że oferowane urządzenia spełniają wymagania określone przez Zamawiającego.

3. **Wymagania szczegółowe minimalne dla sprzętu ujętego w ramach niniejszego przedmiotu zamówienia**

3.1. Przełącznik sieciowy – switch – 1 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Wszystkie przełączniki powinny pochodzić z oficjalnego kanału dystrybucji producenta w Rzeczypospolitej Polskiej. Przełącznik musi być fabrycznie nowy.

L.P.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne**
1.	Obudowa	Obudowa wieżowa 1U umożliwiająca instalację w szafie 19"
2.	Zarządzanie	Telnet, SNMP v1/v2c/v3, Wiersz poleceń (CLI), Przeglądarka WWW

3.	Wejścia / Wyjścia	- RS-232 - min. 1 szt., - 48 portów GE w standardzie 10/100/1000BaseT - 4 porty 1000BaseX ze stykiem definiowanym przez SFP (niezależne od portów miedzianych, nie dopuszcza się tzw. portów Combo) - automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT
4.	Obsługiwane standardy	IEEE 802.1 p, IEEE 802.1 x, IEEE 802.1 Q, IEEE 802.1 w, IEEE 802.1 s, IEEE 802.1 d, IEEE 802.3 x,IEEE 802.3 ad
5.	Rozmiar tablicy MAC	minimum 16000
6.	Obsługa VLAN	Tak. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN
7.	Pamięć	128 MB RAM / 32 MB Flash Przełącznik musi posiadać pamięć DUAL-Flash (możliwość uruchomienia z dwóch różnych wersji obrazu)
8.	Przepustowość	Wydajność przełączania co najmniej 104 Gbps oraz przepustowość 77,3 Mpps dla pakietów 64 bajtowych
10.	Materiał obudowy	metalowy
11.	Parametry i funkcje	Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2 i SNMPv3 Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s) Obsługa Secure FTP Obsługa 802.3ad Link Aggregation Protocol (LACP) Obsługa Simple Network Time Protocol (SNTP) v4 Obsługa LLDP i LLDP-MED (automatyczna konfiguracja VLAN dla telefonów IP). Obsługa zabezpieczeń adresów MAC na portach Zabezpieczenia przed podszywaniem się pod serwer DHCP, (zdefiniowane na konkretny VLAN lub port(y)), Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 4 kolejek sprzętowych, rate-limiting Możliwość autoryzacji użytkowników zgodna z 802.1x Możliwość autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+, 2 Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection) Obsługa list kontroli dostępu (ACL) Obsługa grupowania portów w jeden kanał logiczny zgodnie z LACP (802.3ad)
11.	Gwarancja	Minimum 3 lata Gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniający dostarczenie sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania

		urządzenia oraz wsparcia technicznego. Dodatkowo przez pierwsze 90 dni wymagane jest zapewnienie wsparcia telefonicznego w trybie 24x7.

3.2. Firewall – 1 szt.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowych. Integralność systemu musi być zapewniona także w przypadku różnych dostawców dla poszczególnych lokalizacji. Dopuszcza się, aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

1. System powinien być zaprojektowany w taki sposób, aby możliwa była jego rozbudowa w celu wyeliminowania pojedynczego punktu awarii.

   W tym celu powinien zapewnić, co najmniej:

   1.1. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.

   1.2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

   1.3. Monitoring stanu realizowanych połączeń VPN oraz automatyczne przekierowanie pakietów zgodnie z trasą definiowaną przez protokół OSPF.

   1.4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.

   1.5. System realizujący funkcję Firewall musi dysponować, co najmniej 10 portami Ethernet 10/100/1000 Base-TX

   1.6. Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. W zakresie Firewall'a obsługa nie mniej niż 1250 tys jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę

   1.7. Przepustowość Firewall'a: nie mniej niż 2,8Gbps (dla pakietów UDP 1518/512/64 bajtów)

   1.8. Wydajność szyfrowania 3DES: nie mniej niż 1750 Mbp

   1.9. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:

      1.9.1. kontrola dostępu - zapora ogniowa klasy Stateful Inspection

      1.9.2. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar

      1.9.3. poufność danych - IPSec VPN oraz SSL VPN

      1.9.4. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]

      1.9.5. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.

      1.9.6. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)

      1.9.7. kontrola pasma oraz ruchu [QoS, Traffic shaping]

      1.9.8. Kontrola aplikacji oraz rozpoznawanie ruchu P2P

      1.9.9. Ochrona przed wyciekiem poufnej informacji (DLP)

1.10. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Stateful Firewall, Antivirus, WebFilter, min. 140 Mbps
1.11. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 1200 Mbps
1.12. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
  1.12.1. Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
  1.12.2. Dostawca musi dostarczyć nielimitowanego klienta VPN współpracującego z proponowanym rozwiązaniem (dostępny dla Systemów Microsoft Windows 7 wzwyż, Systemy Android).
  1.12.3. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
  1.12.4. Praca w topologii Hub and Spoke oraz Mesh
  1.12.5. Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF
  1.12.6. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
1.13. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.
1.14. Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
1.15. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
1.16. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
1.17. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
1.18. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
1.19. Ochrona IPS powinna opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać, co najmniej 4000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
1.20. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
1.21. Baza filtra WWW o wielkości co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne (np. spyware, malware, spam, Proxy avoidance). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
1.22. Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
1.23. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
  1.23.1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
  1.23.2. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
  1.23.3. haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
  1.23.4. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.

1.24. Funkcje bezpieczeństwa oferowanego systemu powinny posiadać certyfikaty ICSA dla funkcjonalności Firewall, IPS, Antywirus

1.25. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami wchodzącymi w skład systemu. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

Wymaga się, aby dostawa obejmowała również:

- Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 36 m-ce
- 36 miesięczny Serwis logistyczny na terenie Polski z dostawą urządzenia zastępczego na drugi dzień roboczy / 8x5xNBD gwarantujący udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy w Następnym Dniu Roboczym.

1.26. Gwarancja oraz wsparcie

1) Gwarancja: Dostarczone elementy systemu powinny być objęte serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.

2) Gwarancja/AHB/SOS: System powinien być objęty rozszerzonym serwisem gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin/, realizowanym przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego, mającego swoją siedzibę na terenie Polski.

Dla zapewnienia wysokiego poziomu usług podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w trybie 8x5 / 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię 8x5 /24x7.

Oferent winien przedłożyć dokumenty:

- oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej
- oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej)
- certyfikat ISO 9001 podmiotu serwisującego

3) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego

systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

4) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

4. Wymagania dotyczące gwarancji

Dostarczone, zainstalowane i uruchomione urządzenia mają być objęte przynajmniej 3-letnią gwarancją (chyba, że w formularzu ofertowym załączniku nr 1 Zamawiający wymaga innego okresu gwarancyjnego), świadczoną na miejscu u klienta z czasem reakcji serwisu - do końca następnego dnia roboczego.

Okres gwarancji liczony będzie od dnia odbioru całego zainstalowanego i uruchomionego systemu. Szczegółowy zakres gwarancji został ujęty w SIWZ i w Umowie.

Dostarczone przez Wykonawcę urządzenia zostaną podłączone do zasilania udostępnionego przez Zamawiającego.

Zamawiający dopuszcza zastosowanie urządzeń, technologii oraz programów równoważnych innych niż określone w SIWZ. Ciężar udowodnienia, że urządzenia oraz oferowana technologia jest równoważna w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy.

Urządzenia równoważne muszą pracować w tej samej technologii co urządzenia określone w dokumentacji.

Załącznik 8.5. do SIWZ – OPZ dla Części III – Gmina Żórawina

1. **Zestawienie zbiorcze sprzętu w ramach części III - Dostawa infrastruktury sieciowej – aktywnej i pasywnej**

Część III – Dostawa infrastruktury sieciowej – aktywnej i pasywnej		**Gmina Żórawina**
L.p.	**Rodzaj sprzętu**	**Ilość sztuk**
1.	Switch zarządzalny	1

2. **Wymagania generalne dla dostaw i usług związanych z niniejszą częścią zamówienia**

W zakresie realizacji niniejszych wymagań OPZ przewiduje się:

- Dostawę, instalację, konfigurację i uruchomienie zgodnie ze wskazaniem Zamawiającego urządzenia wymienionego w poz. 1 powyższej tabeli.

Wszystkie wskazania z nazwy urządzeń występujących w szczegółowym opisie przedmiotu zamówienia należy rozumieć, jako określenie wymaganych minimalnych parametrów technicznych lub standardów jakościowych. Oznacza to, że zgodnie z art.29 ust.3 ustawy Prawo zamówień publicznych wskazaniom tym towarzyszą wyrazy „lub równoważne". Wykonawca, który w ofercie powoła się na zastosowanie urządzeń równoważnych opisanych w SIWZ, jest obowiązany wykazać, że oferowane urządzenia spełniają wymagania określone przez Zamawiającego.

3. **Wymagania szczegółowe minimalne dla sprzętu ujętego w ramach niniejszego przedmiotu zamówienia**

3.1. Przełącznik sieciowy – switch – 1 szt.

Właściwości	**Wymagane parametry minimalne**
Obudowa:	typu RACK 1U
Zarządzanie:	Telnet, SNMP v1/v2c/v3, Wiersz poleceń (CLI), Przeglądarka WWW
Wejścia/wyjścia:	RS-232 - min. 1 szt., RJ-45 10/100/1000 Mbps - min. 24 szt., min. SFP - 4 szt.
Obsługiwane standardy:	IEEE 802.1 p, IEEE 802.1 x, IEEE 802.1 Q, IEEE 802.1 w, IEEE 802.1 s, IEEE 802.1 d, IEEE 802.3 x,IEEE 802.3 ad
Rozmiar tablicy MAC:	8 k
Pamięć: min.:	128 MB RAM, min. 32 MB Flash
Algorytm przełączania:	Store-and-forward
Przepustowość	min 35 Mpps
Warstwa przełączania:	2
Materiał obudowy:	metalowy
Dołączone akcesoria:	kabel zasilający do sieci 230V

4. **Wymagania dotyczące gwarancji**

Dostarczone, zainstalowane i uruchomione urządzenia mają być objęte przynajmniej 3-letnią gwarancją (chyba, że w formularzu ofertowym załączniku nr 1 Zamawiający wymaga innego okresu gwarancyjnego), świadczoną na miejscu u klienta z czasem reakcji serwisu - do końca następnego dnia roboczego.

Okres gwarancji liczony będzie od dnia odbioru całego zainstalowanego i uruchomionego systemu. Szczegółowy zakres gwarancji został ujęty w SIWZ i w Umowie.

Dostarczone przez Wykonawcę urządzenia zostaną podłączone do zasilania udostępnionego przez Zamawiającego.

Zamawiający dopuszcza zastosowanie urządzeń, technologii oraz programów równoważnych innych niż określone w SIWZ. Ciężar udowodnienia, że urządzenia oraz oferowana technologia jest równoważna w stosunku do wymogu określonego przez Zamawiającego spoczywa na Wykonawcy.

Urządzenia równoważne muszą pracować w tej samej technologii co urządzenia określone w dokumentacji.